Security and Privacy of Things: Regulatory Challenges and Gaps for the Secure Integration of Cyber-Physical Systems

Geraldine Lee[1], Gregory Epiphaniou[2], Haider Al-Khateeb[2], and Carsten Maple[3]

[1] QA Ltd, Slough, Berkshire, UK
geraldine.lee@qa.com
[2] Wolverhampton Cyber Research Institute (WCRI), School of Mathematics and Computer Science, University of Wolverhampton, Wolverhampton, UK
g.epiphaniou@wlv.ac.uk, h.alkatheeb@wlv.ac.uk
[3] WMG Group, University of Warwick, Coventry, UK
cm@warwick.ac.uk

Abstract. The rise of interconnected "intelligent" objects that move their capabilities from sensing and data processing to decision-making will be a disruptive phenomenon that further widens the gaps between legal, regulatory and technological approaches. This research sets out to establish a guided roadmap through the maze of regulation by incorporating the fragmented governance efforts into a single focus where security and privacy gaps unique to Machine-to-Machine communication (M2M) are identified against key performance metrics. We use privacy, ethics, trust, legality, data sharing, operational integration and device and communication protocols as our key performance metrics to highlight areas of significant overlap and gaps in a comprehensive list of standards to assist policymakers and researchers in the field. Results also indicate that policy concerns and diffused responses from existing standards raise unacceptable risks for the cyber and physical spheres in the IoT preventing their integration with existing hierarchical security architectures and reducing the opportunities for mass-market economies of scale.

Keywords: Internet of Things, Machine-to-Machine, Cyber-Physical Systems, Governance

1 Introduction

Cyber-Physical Systems (CPS) seek to integrate physical and computational processes. Certain characteristics of CPS include but not limited to integrated computation, and physical processes with resource-constrained physical components, massive scale network infrastructures and a large variety of devices and system types [19]. The necessity to re-organise and re-configure their existing capabilities requires a high degree of automation to favour human-to-machine

(H2M) communications. Unfortunately, the speed at which technology is progressing surpass regulatory and legal control. Both industry and society forces demand further benefits from the Internet of Things (IoT) technology with an exponential acceleration of M2M communication [3]. The current response of legal and regulatory bodies is rather slow leading to an absence of holistic and adequate standards, guidelines and frameworks. There is currently a maze of developing rules, regulations and frameworks applicable to M2M [18], [7]. With the proliferation of smart devices and the evolution of networked CPS historically contained within industrial systems alongside with IoT devices, there is a systematic increase in dependencies between the physical, natural and cyber domains [9]. The transparency in the interactions between a person and a system has established a suitable level of complexity suppressing more complicated details of this interaction which is a core characteristic of IoT and M2M communications [5]. Adding to this complexity is the vague and ambiguous meaning of IoT at different levels of abstractions throughout the supply chain from semi-conductors to service providers where different visions and multi-disciplinary activities coexist. These activities expand further the necessity for intelligence-driven security operations where continuous monitoring of the networks and proactive network defence with strict guidelines and technical standards are required [17]. There is an undisputable number of benefits by both users and providers from M2M communications and IoT technologies that can only be exploited when challenges unique to IoT and M2M are fully addressed [4],[6].

The remainder of this paper is structured as follows: Section 2 presents a systematic review of existing governance and compliance standards with references to security, privacy and trust requirements and links to the IoT/M2M paradigm. Section 3 presents our partially articulated roadmap with clear mappings on existing overlaps and gaps in regulatory and compliance standards, frameworks and codes of conduct with regards to CPS and M2M communications. Finally, Section 4 concludes this paper.

2 Standardisation in IoT

With the vast proliferation of physical devices in fully networking environments several issues around security over their lifetime have risen. Patch management, updating and configuration of sensors as well as local and remote diagnostics have become more arduous with energy efficiency from the security operations a key stake at hand particularly in the context of sensor networks [1]. Challenges in governance and management of data generated, shared and collected by sensors and smart devices with emphasis on data accessibility have also raised. Existing data seems to be rich with time stamping and other metadata enabling inference or aggregation attacks revealing information more sensitive and valuable than the raw data. ISO/IEC 27010:2015 [2] raises the need for information classification to include the credibility, value and level of trust to the information collected and shared. Given that specific smart devices and sensors are being used increasingly in domestic environments privacy concerns have also noted as

part of their operation. The authors in [8] also lament that privacy is seen by organisations as a legal issue and security a technical issue with stakeholders rarely collaborating to achieve both goals.

The UK Information Commissioners Office (ICO) has issued specific guidance documents related to the EU General Data Protection Regulation (GDPR). The guidance states that GDPR for EU IoT purposes indicates unambiguous gaining of consent and clear affirmative actions which are also a key within ISO/IEC 29100:2011 [12], [10]. There is a definite directive therein that requires personally identifiable information (PII) controllers to obtain opt-in consent and choice of the PII principal with full transparency on the collection and use of their PII.

The privacy by design element is outlined as a core component and best practice in any activities within which PII collection and processing takes place with Privacy Impact Assessment(s) (PIA) playing a key role as part of this practice. In ISO/IEC DIS 29134:2017 privacy impact assessment guidelines [16] and ISO29134, PIA has been described further as a systematic process rather than a tool particularly relevant when digitally connected devices are part of the Information system or components of applications being tested.

Although DPA or GDPR do not explicitly apply to M2M communication, fundamental principles may be adopted by existing and future standards and frameworks. In the context of M2M, a number of PII controllers may exist when PII is transferred or shared adding layers of complexity.

ISO/IEC 29182-1:2013 also recommends sensor networks should ensure user privacy as sensed data could be sensitive and contain personal information.

ISO/IEC 27018:2014 [13] can be used as an instructive element to the broader IoT spectrum as it emphasises on the protection of PII in public Clouds who act as PII processors. Aforementioned is particularly interesting given the provision of mature Cloud services has been seen as an enabling infrastructure to support M2M. ISO 27010 also addresses concerns around sensitive information with an emphasis on sharing between inter-sector or inter-organisation. Within its Annex B informative guidance is given on the provision of trust and reputation engines in information filtering and sharing. The quality of the information upon which decisions are made can be significantly affected by the current de-regulated sharing activities. Despite these developments, M2M/IoT is not explicitly considered. However, information from the standard acts as a tailor to the security controls within ISO/IEC 27002:2013. The necessity to identify and address emerging security challenges raised by technological evolution in M2M communications has been acknowledged fully.

ISO/IEC 38500:2015 [14] emphasises to the IT governance of organisation with elements around decision making and processes related to IT usage. Although there are no direct references or links to M2M, this standard seems to provide a good basis and guidance around legal, regulatory and ethical considerations. A systematic overview of managing non-compliance risks arising from IT misuse is also covered. Several internal and external drivers in political, commercial and social contexts must also be considered when M2M and IoT are concerned. In ISO/IEC 31000:2009 there is a clear outline of the require-

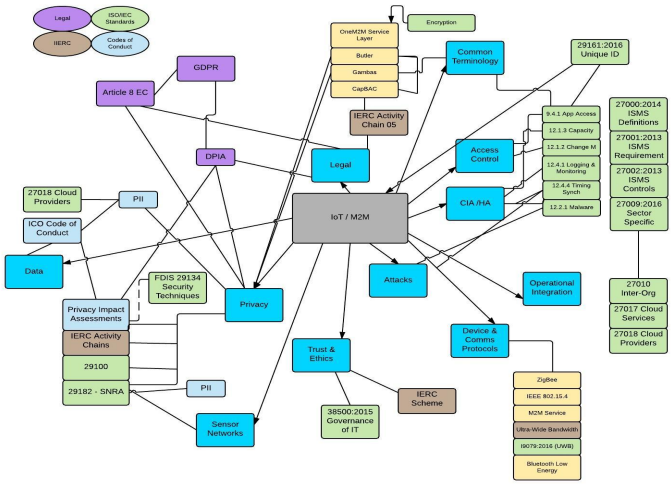

Fig. 1. Existing Legal and Regulatory compliance efforts and their relationship to IoT/M2M

ments the needs of interested parties and stakeholders and the interfaces and dependencies between activities in both isolated or in the broader context of cross-organisational communications.

In ISO/IEC 27009:2016 [15] the sector-specific requirements based on application or market have been defined in alignment with ISO27001. A comprehensive set of controls has been provided related to information management for inter-sector and inter-organization communications with further references to PII protection as outlined in 27010:2015 and ISO27018 controls. Unfortunately, there is no indication as yet of the design or development of suitable controls to M2M/IoT. Finally, some links to IoT established through information within ISO/IEC 24760-1:2011 [11] where a framework for identity management, data processing and decision-making and information gathering is defined. The standard defines an entity as an item inside or outside information and communication technology system(s), e.g. a person, device, organisation or subsystem which can be potentially useful in the IoT paradigm.

3 Towards a Roadmap for Secure CPS Integration

An extensive range of standards and frameworks with an effort to establish links between their legal and regulatory compliance relevant to M2M and IoT is illustrated in Figure 1. These links are based on domains of governance and categories of key performance metrics (KPM) as identified in the public domain (see appendix A). Controls from ISO 27002 relevant to M2M also have been selected with the main sources of governance classified in our work as ISO/IEC standards, DIS ISO/IEC standards (draft), Codes of Conduct, Legal frameworks,

Table 1. Colour Coding System Used in Section 3.1

Key	Indication
	Key areas of concentration and overlapping responses within categories and KPIs are indicated
	Minimal responses or complete absence or gaps in response to address the categories and the KPIs are indicated

IERC projects and Low Power Communication guidelines. These domains of governance have been selected to represent a broad range of International and European guidance within the public, commercial, information security, legal and technological sectors.

Our roadmap is articulated through the development of Standards, Codes of Conduct, legal provisions and additionally a number of projects within the IERC and utilises existing standards and frameworks within the categories of user privacy, sensor networks, legal, ethics, common terminology, access control and high availability, data, attack vectors and trust.

3.1 Results and Discussion

Table 1 clearly presents the colour coding scheme used this section to illustrate key areas of concentration in the governance domains and areas where there appears to be a lack of standards response. The use of x indicates which KPM has been addressed. Table 2 illustrates the broader issue of consent across all domains of interest and an acknowledgement that use privacy must be taken seriously under consideration in the development of governance controls. At first glance, this observation is particularly relevant to IoT as there is a significant amount of PII and sensitive information to be captured irrespectively to user/sensor location and the boundaries of the Information security management system (ISMS). With regards to trust in sensor networks in ISO29182-1:2013 elements such as node discovery and sensor node capability detection are considered. However, credibility and trustworthiness of these nodes are overlooked as the credibility of these nodes are not dictated by the standard and left as informative actions in ISO27010 or as an extension part in ISO29182.

Table 3 illustrates that data is mostly overlooked unless considered sensitive in which case ISO27010 addresses it. Sensitive data is only considered within ISO27010 and therefore presents a gap in the domains. Increasingly, sensitive and confidential information is being held on smart devices and despite campaign groups seeking protection of such information from disclosure, there is an absence of legal response. Elements around differential privacy and patterns of behaviour/ aggregation are not addressed in any domain. Aforementioned represents a substantial gap which must be addressed if M2M/IoT initiatives are to be successful, especially in applications such as Intelligent Transport Networks. Despite the use of anonymised data, privacy can be compromised by the use of auxiliary data collected including browsing habits.

Substantial gaps have also been identified in the existing standards with regards to smart device decision-making and control (See Table 4). In the complete absence of trust and preferential privacy controls the need safeguard and regulate decisions based on sensors/devices as trusted sources are of paramount importance. That becomes a more pressing issue in cases of inference attacks or revealing PII or user behaviour in a given context. Our mapping exercise also suggests a complete absence of controls relating directly to operational integration within M2M/IoT. That is a significant challenge which must be addressed. As devices in the field increase with minimal ability to patch and update the threat landscape increases.

In the context of M2M, the mobility of nodes and nodes' participation in the network mainly, those which run on a battery will be diverse. This standard addresses these metrics but indicates them as optional. Furthermore, M2M/IoT is likely to require responsiveness to changing environments with devices deployed in the field and as such according to ISO29182 may need self-organising and self-healing capabilities. As devices tend to be geographically distributed, network management and service discovery should also constitute core capabilities of these infrastructures. Unfortunately, in their current form, these capabilities are regarded as optional. The results presented in this section demonstrate that although the critical areas of focus are observed in some governance domains, there is no one approach that addresses, trust, privacy, ethics, operational integration and integrity, device and communication protocols and Sensor Networks. On the contrary, the existing plan seems to be scattered and confused proving that although there is a variety of standards relevant to the IoT, currently, there is lack of coordination between them.

4 Conclusion

This work partially articulates an assurance roadmap incorporating architectural components related to governance domains, categories of challenges raised with M2M and IoT together with key areas of focus represented as a set of key performance indicators. Our work confirms that there is a need for continued research into this area with a more granular focus and analysis of M2M and IoT governance challenges. This work is necessary to demonstrate that the diffuse responses and standards maze raise unacceptable security risks for the cyber and physical spheres of the IoT. Having demonstrated the overlaps and gaps in existing standards, future work should seek to exploit the strengths in current efforts to develop a set of guidelines for secure integration across the full end to end M2M paradigm.

Table 2. Performance metrics of Consent and Choice mapped to Domains

KPI	29161:2016	29182-1:2013	24760-2:2011	27018:2014	27001:13 / 27002:2013	27010:2015	27017:2015	29100:2011	29134	38500:2015
User Privacy Consent and Choice		x Recommended		x				x x		x
	x GDPR	x Article 8	x GAMBAS	x BUTLER	CapBAC	M2M Service Layer				

Table 3. Category of Data Mapped to ISO/IEC Standards, Codes of Conduct, Legal Frameworks and IERC Projects

ISO/IEC	29161:2016	29182-1:2013	24760-2:2011	27018:2014	27001:13 / 27002:2013	27010:2015	27017:2015	29100:2011	29134	BS ISO/IEC 38500:2015	(Data) Privacy Impact Assessment (PIA) (DPIA)	GDPR	Article 8 EC Human Rights	GAMBAS	BUTLER	CapBAC	M2M Service Layer
Categories and KPI's	Data structure - Unique Identification for the Internet of Things	Sensor Network Reference Architecture (SNRA) Part 1: General overview and requirements	A framework for identity management. Part 1: Terminology and concepts	Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors.	Information security management systems - Requirements	Information security management for inter-sector and inter-organizational communications	Code of practice for information security controls based on ISO/IEC 27002 for cloud services	Privacy framework	Privacy impact assessment - Guidelines	Governance of IT for the organization							
Data Transparency							38100				x	x		x	x		
Consent											x	x		x	x		
Erasure											x	x					
Ownership											x						
Anonymity / soft identities						x								x			
User defined access control policy														x	x		
Encrypted queries														x			
Accuracy											x				x		
Differential Privacy																	
Sensitive Data Handling						x											x
Sensitive Data						x											x

Table 4. Metrics of Smart Device Decision Making and Control; & Low Power Communication mapped by domain

Low Power Communication					ISO/IEC	IERC Projects		
	ZigBee	IEEE 802.15.4	Bluetooth low energy (LE)	Ultra-Wide Bandwidth (UWB)	RFID/NFC	BS ISO 19079:2016	29182-1:2013	OneM2M Org
KPI's						Intelligent Transport Systems - Communications access for land mobiles (CALM) 6LoWPAN networking	Sensor Network Reference Architecture (SNRA) Part 1: General overview and requirements	M2M Service Layer
Device & Communication Protocols								
OSI Layers								
Physical		x						
DataLink		x				x		
Network	x					x		
Transport	x							
Application	x							x
Low power / energy management		x	x	x	x		x May Require	x
Key Distribution							x Required	
IPSEC (AH, ESP)						x		
Host to Host C, I		x						
End to End C,I,A						x		
Secure Mac Headers								
QOS							x May Require	
Encryption							x May Require	
TLS/DTLS								x

References

[1] (2013) Iso/iec 29182-1:2013 - information technology – sensor networks: sensor network reference architecture (snra) – part 1: general overview and requirements_2013. URL https://www.iso.org/standard/45261.html

[2] (2015) iso/iec 27010:2015 - information technology – security techniques – information security management for inter-sector and inter-organizational communications_2015. URL https://www.iso.org/standard/68427.html

[3] Abdul-Qawy AS, J PP (2015) The internet of things (iot)&58; an overview. International Journal of Engineering Research and Applications 5(12)

[4] Atzori L, Iera A, Morabito G (2010) The internet of things: A survey. Comput Netw 54(15):2787–2805, DOI 10.1016/j.comnet.2010.05.010, URL http://dx.doi.org/10.1016/j.comnet.2010.05.010

[5] Babar SD, Prasad NR, Nielsen RH, Alam M, Chen K (2016) Multi-disciplinary applications requiring advanced iot and m2m. Role of ICT for Multi-Disciplinary Applications in 2030 47:23

[6] Baldini G, Botterman M, Neisse R, Tallacchini M (2016) Ethical design in the internet of things. Science and Engineering Ethics DOI 10.1007/s11948-016-9754-5, URL https://doi.org/10.1007/s11948-016-9754-5

[7] Boswarthick D, Elloumi O, Hersent O (2012) M2M communications: a systems approach. John Wiley & Sons

[8] Herold R, Hertzog C (2015) Data Privacy for the Smart Grid. Auerbach Publications, URL https://www.amazon.com/Data-Privacy-Smart-Rebecca-Herold/dp/1466573376?SubscriptionId=0JYN1NVW651KCA56C102&tag=techkie-20&linkCode=xm2&camp=2025&creative=165953&creativeASIN=1466573376

[9] Hsu DF, Marinucci D (2012) Advances in cyber security: technology, operations, and experiences. Oxford University Press

[10] ICO (2016) Preparing for the general data protection regulation (gdpr). URL https://ico.org.uk/media/1624219/preparing-for-the-gdpr-12-steps.pdf

[11] ISO (2011) Iso/iec 24760-1:2011 information technology – security techniques – a framework for identity management – part 1: Terminology and concepts. URL https://www.iso.org/standard/57914.html

[12] ISO (2011) Iso/iex 29100:2011 information technology – security techniques – privacy framework. URL https://www.iso.org/standard/45123.html

[13] ISO (2014) Iso/iec 27018:2014 information technology – security techniques – code of practice for protection of personally identifiable information (pii) in public clouds acting as pii processors. URL https://www.iso.org/standard/61498.html

[14] ISO (2015) Iso/iec 38500:2015 information technology – governance of it for the organization. URL https://www.iso.org/standard/62816.html

[15] ISO (2016) Iso/iec 27009:2016 information technology – security techniques – sector-specific application of iso/iec 27001 – requirements. URL https://www.iso.org/standard/42508.html

[16] ISO (2017) Iso/iec 29134:2017 information technology – security techniques – guidelines for privacy impact assessment. URL https://www.iso.org/standard/62289.html

[17] Lee J, Bagheri B, Jin C (2016) Introduction to cyber manufacturing. Manufacturing Letters 8:11–15

[18] Paez M, La Marca M (2016) The internet of things: Emerging legal issues for businesses. N Ky L Rev 43:29

[19] Shi J, Wan J, Yan H, Suo H (2011) A survey of cyber-physical systems. In: 2011 International Conference on Wireless Communications and Signal Processing (WCSP), pp 1–6, DOI 10.1109/WCSP.2011.6096958

A Appendix

Table 5: Key performance metrics and Sub-Categories

User Privacy	**Data**
Human Factors /People in the Process	Transparency
Time stamped data	Consent
PIA / Risk Assessment	Erasure
Personally Identifiable Information (PII)	Ownership
Consent and Choice	Anonymity / soft identities
Collection Limitation	User defined access control policy
Data minimization	Encrypted queries
Use, retention and disclosure limitation	Accuracy
Openness, transparency and notice	Differential Privacy
Individual participation and access	Sensitive Data Handling
Information asset	Sensitive Data
Privacy safeguarding	
Control objectives	Attacks
External/Contractual Stakeholders	Timing attacks - reflection attacks, manipulation)
	Device based attacks
Legal	
Risk Management	
	Device & Communication Protocols
Financial Penalties	OSI Layers
	Physical
Common terminology	Data Link
Definition of Thing / Entity / Object	Network
Unique Identification of Thing	Transport
URI (URL or URN)	Application
Modular Design	Low power / energy management
Patterns of behaviour / aggregation	Key Distribution
	IPSEC (AH, ESP)
Ethics	Host to Host Confidentiality, Integrity (C,I)
Smart device decision making/control	End to End C,I, Availability (CIA)
	Secure Mac Headers
Trust	Quality of Service (QOS)
	Encryption
Operational integration and integrity	Transport Layer Security , Datagram TLS (TLS/DTLS)
Components in field	Time Synchronization
Geographic dispersal of sensors	
Updates/patches	
	Sensor Networks
	Connectivity to other networks
Access Control	Observe/Acquire information about physical world
Subject/Object Level	Node Mobility
Access Control Lists	Dynamic Topology
Role Based Access Controls (RBAC)	Self Organizing / Healing
	Context Awareness
CIA and High Availability	Scalability
Confidentiality	Sensor Network Management
Integrity	Sensor Node Discovery
Availability	Sensor Node Capability Discovery
Authentication	Service Discovery
Reliability	Routing
Capacity	Inputs/Outputs to Physical Environment
Information Security Management System (ISMS) & Security Controls	
Continuity	
Continual Service Improvement	
Event Management	
Reliability	